OFFICE OF INSPECTOR GENERAL

EVALUATION REPORT

FISCAL YEAR 2009 EVALUATION OF NEA'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002

REPORT NO. R-10-02, rev. 2/26/10
JANUARY 22, 2010

REPORT RELEASE RESTRICTION

In accordance with Public Law 110-409, The Inspector General Act of 2008, this report shall be posted on the National Endowment for the Arts (NEA) website not later than three (3) days after it is made publicly available with the approval of the NEA Office of Inspector General. Information contained in this report may be confidential. The restrictions of 18 USC 1905 should be considered before this information is released to the public. Furthermore, information contained in this report should not be used for purposes other than those intended without prior consultation with the NEA Office of Inspector General regarding its applicability.

INTRODUCTION

The Federal Information Security Management Act of 2002 requires an annual evaluation by the Inspector General on its agency's information security programs and practices. This report presents the results of our evaluation of NEA's information security program and practices for protecting its information technology (IT) infrastructure.

BACKGROUND

The Federal Information Security Management Act (FISMA) of 2002 was signed into law on December 17, 2002. It replaced the *Government Information Security Reform Act* (GISRA), which expired in November 2002. The Act requires each federal agency to develop, document, and implement an agency-wide information security program to provide information security over the operations and assets of the agency. This includes:

- Periodic risk assessments;
- Policies and procedures that are based on risk assessments;
- Subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;
- Security awareness training to inform employees (including contractors) of the security risks associated with their activities and their responsibilities to comply with those agency policies and procedures designed to reduce those risks;
- Periodic testing and evaluation of the effectiveness of information security policies;
- A process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices, of the agency;
- Procedures for detecting, reporting, and responding to security incidents; and
- Plans and procedures to ensure continuity of operations of the agency's information systems.

Office of Management and Budget (OMB) Memorandum M-09-29, dated August 20, 2009, entitled *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, updates instructions to Senior Agency Officials for Privacy, Chief Information Officers and Inspectors General for reporting their 2009 information to OMB. Although the requirements changed little this year, reporting was accomplished through an automated collection tool.

The National Institute of Standards and Technology (NIST), which has the responsibility for developing technical standards and related guidance, has issued numerous publications including NIST Publication 800-12 *An Introduction to Computer Security: The NIST Handbook*. This publication explains important concepts, cost considerations, and interrelationships of security controls as well as the benefits of such controls. NIST

also has published a *Guide for Developing Security Plans for Information Technology Systems*; Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*; Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*; and FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems.* In addition, guidance is found in the Government Accountability Office publication, *Federal Information System Controls Audit Manual* (FISCAM).

NEA's Office of Information and Technology Management (ITM) maintains and operates two of the Agency's three core systems on a local area network (LAN). These are the Grants Management System (GMS), which contains information on grant applications and the Automated Panel Bank System (APBS), which contains information on panelists who review grant applications. NEA has contracted with the Department of Transportation Enterprise Service Center to host NEA's Financial Management System (FMS) through its Delphi Financial Management System. In addition, NEA operates support systems including electronic mail, and internet and intranet services.

The Chief Information Officer (CIO) is responsible for developing policies and procedures to ensure that security is provided over NEA's networks.

OBJECTIVE AND SCOPE

The objective of the evaluation was to determine the adequacy of NEA's information technology (IT) security program and practices. This included a review of NEA's IT security policies and procedures and privacy management program. It also included interviews with responsible agency officials managing the IT systems, and tests on the effectiveness of security controls.

PRIOR EVALUATION

The NEA Office of Inspector General (OIG) issued a report entitled *Fiscal Year 2008 Evaluation of NEA's Compliance with the Federal Information Security Act of 2002* (Report No. R-09-02) dated October 9, 2008. The report had six (6) recommendations, of which two, Recommendations Nos. 1 and 2 remained open at the time of our review. However**, s**ubsequent to the exit conference, ITM submitted documentation to the OIG confirming the corrective action for Recommendation No. 1 was completed. *Based on the documentation provided, the NEA Audit Follow-up Official cleared this recommendation*.

The status of the remaining recommendation is summarized below.

Recommendation No. 2

ITM should revise the Continuity of Operations Plan (COOP) to address the deficiencies noted in the SeNet report.

ITM submitted a draft of the revised COOP addressing the deficiencies noted in the SeNet report; however, the draft did not include a list of Vital Records and Databases as required. *This recommendation will remain open until ITM provides the OIG a completed and approved COOP.*

EVALUATION RESULTS

The FY 2009 evaluation concluded that there are several issues that need to be addressed by NEA's Office of Information and Technology Management. These issues are related to the Security Plan, ITM policies, the security certification and accreditation of the information network, reporting of Plans of Action and Milestones (POA&Ms) on the quarterly FISMA reports, inventory control and change management. Details are presented in the following narrative.

Security Plan

The development of security plans are an important activity in an Agency's information security system that directly supports the security accreditation process required under FISMA and OMB Circular A-130, *Management of Federal Information Resources.* Security plans should ensure that adequate security is provided for all Agency information collected, processed, stored, or disseminated in NEA's general support systems and major applications.

ITM last revised the NEA Security Plan in June 2007. During our FY 2008 FISMA review, we found the security plan had not been revised although there were several system changes which should have been incorporated. At that time, ITM informed us that the Security Plan was being updated. During the current review, we again found that the Security Plan had not been updated. Subsequent to the exit conference, ITM informed us that the security plan is being revised in accordance with federal guidelines and would also encompass all ITM policies.

We recommend that ITM complete and approve the Security Plan as required by its *Standard Procedures for Developing Information Technology Policies.* A copy of the approved Security Plan should be provided to the OIG.

ITM Policies

During the FY 2008 evaluation, we found ITM policies which (1) were not updated to reflect current security requirements, (2) did not include a date of issuance or (3) were issued without formal approvals. We recommended that ITM implement standard procedures for developing policies to ensure that only approved policies are issued and that those policies are made available to employees. ITM provided us a copy of the "Standard Procedures for Developing Information Technology Policies," which are

instructions for developing ITM policies and making those policies available to employees. The instructions were approved by the Chief Information Officer.

During this evaluation, we determined that the instructions for developing ITM policies had not been effectively implemented. We again found policies that were not approved, revised or made available to employees. For example, ITM has several policies posted on its intranet website; however, we found several inactive links for policies such as Audit & Accountability Policy and the Security Awareness Training Policy, both of which, according to ITM, are a part of the Security Plan. In some cases, policies on the intranet had not been updated.

The following policies should be revised and authorized per the ITM "Standard Procedures for Developing Information Technology Policies":

- Site Certification and Accreditation Policy
- System Security Plan

ITM does not have policies for Inventory Controls and Contractor Security; therefore, we recommend that ITM develop and implement policies addressing these areas. We also recommend that ITM implement its standard procedures for developing all policies, and make those policies available to employees.

Security Certification and Accreditation (C&A)

ITM certified its Information Network supporting the National Endowment for the Arts in its March 2006 *National Endowment for the Arts Information System Network Site Certification and Accreditation*. The Network consists of the Grants Management System and Automated Panel Bank System. It is authorized to process information that is "sensitive," but unclassified. The NEA Information System Network is connected to the National Finance Center (NFC) and the Department of Transportation – Federal Aviation Administration – Aeronautical Center, Enterprise Service Center. The accreditation was valid for three years or until March 2009. As of our review in August 2009, the C&A had not been performed.

We recommend that ITM perform the security certification and accreditation review on all its systems as required.

NIST Self-Assessment and Plans of Action and Milestones (POA&Ms)

An external risk assessment was performed in FY 2008; therefore a self-assessment is not scheduled to be performed until December 2009. However, as part of our evaluation we reviewed the quarterly FISMA reports submitted to OMB. We reviewed the reports to determine whether ITM was reporting all its POA&Ms which were unresolved more than 90 to 120 days beyond the planned remediation date) as required by OMB:

We noted that the following POA&Ms were reported during FY 2009:

	Number of POA&Ms
• December 2008	0
• March 2009	3
• June 2009	1

In each case, the weaknesses were regarding the COOP. However, during our review we found several unresolved POA&Ms which were more than the 90-120 days beyond the remediation period such as the revisions and/or approvals of policies. For instance, the "Security Plan" policy had not been updated and approved since the prior evaluation; therefore it should have been reported on the quarterly FISMA report.

We recommend, as we have in prior reviews that ITM include all POA&Ms, which are more than *90* days beyond the planned remediation date, in its quarterly FISMA report as required by the Office of Management and Budget.

Privacy Reporting and Privacy Impact Assessment

The 2009 FISMA guidance included additional questions on security and privacy policies, which requires agencies to submit information on privacy issue allegations, policies and the types of privacy reviews ITM conducted. OMB directed agencies to submit their most current documentation related to OMB Memorandum M-07-16, of May 22, 2007, "*Safeguarding Against and Responding to the Breach of Personally Identifiable Information*," (PII). OMB Memorandum M-07-16 requires agencies to review their use of SSNs, in agency systems and programs, in order to identify instances in which collection or use is superfluous.

To comply with the requirements above, NEA's ITM has:

- Implemented PII policies regarding breach notification and rules of behavior;
- Completed technical security assessments to evaluate the level of security *protecting NEA IT assets;*
- Reviewed PII holdings and updated the system of records notice to include OMB recommended "routine uses" of PII language; and
- Modified security orientation and privacy training for all NEA staff to include responsibility to protect Agency information and technology assets.

ITM's review of PII holdings determined that NEA collects only PII that is relevant and necessary for administrative purposes and determined that there are adequate administrative, technical and physical safeguards in place for the PII collected. NEA does not use Social Security Numbers (SSNs), truncated SSNs, or any part of SSNs as tracking numbers for its applications, grants, cooperative agreements or contracts. NEA

does not share PII with outside agencies other than for processing payments. ITM indicated there have been no reported breaches or security incidents involving PII collected or maintained by the Agency. ITM also indicated that there were no changes to the policy since the 2008 FISMA status report on PII and SSNs which was issued September 18, 2008.

IT Security and Privacy Awareness Training

NIST Special Publications 800-50, *Building an Information Technology Security Awareness and Training Program* and 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, provide the standards for security awareness and training. ITM combined *IT Security and Privacy Awareness Training* in the FY 2008 Annual Refresher Training. The FY 2009 annual training also included reporting computer incidents.

We obtained and reviewed the list of employees who had completed the FY 2009 security awareness training and determined that 98% of the staff completed the required *Annual IT Security and Privacy Awareness Refresher* training on security awareness and privacy (172 completed, 4 did not complete).

Inventory Controls

NEA has an inventory of its hardware that was updated as of July 17, 2008. The perpetual inventory listing is maintained and updated as equipment is added or deleted. The inventory lists each item by office, barcode number, serial number, manufacturer, model number and description, as well as the user. It also indicates the date the inventory was taken and the initials of the person who took the inventory. During this review we were advised the inventory for FY 2009 was in process. However, subsequent to our review ITM provided the OIG a copy of the 2009 inventory.

We recommend that ITM develop policies and implement procedures to ensure that the ITM inventory is completed annually.

Change Management

ITM issued a *Change Management Policy/Procedure* in 2005. This policy "describes the responsibilities, policies, and procedures to be followed by ITM when making changes or recording events to the National Endowment for the Arts IT infrastructure." It defines "change" and "event" as follows:

> **Change: to transform, alter, or modify the operating environment or standard operating procedures; any modification that could have potential and/or significant impact on the stability and reliability of the infrastructure and impacts conducting normal business operation by our users and ITM; any interruption in building environments (i.e., electrical outages) that may cause disruption to the IT infrastructure.**

Event: any activity outside of the normal operating procedures that could have a potential and/or significant impact on the stability and reliability of the infrastructure, i.e. a request to keep a system up during a normal shutdown period.

The change management process includes the submission of a change request form, with management approval, to the Information System Security Officer (ISSO). During our FY 2008 evaluation, we noted that although there were changes made to the system, no request forms had been submitted to the ISSO. As a result, we recommended that ITM implement procedures to ensure compliance with the *NEA Change Management Policy/Procedure*. This year, we again requested copies of completed change management request forms and found that no submissions had been made.

We recommend that ITM revise, approve and implement the *NEA Change Management Policy/Procedure* as required by its *Standard Procedures for Developing Information Technology Policies.* We also recommend that the CIO direct staff to adhere to those procedures.

During the exit conference, the CIO stated that he had directed the staff to adhere to the change management policy on January 14, 2010.

Financial Management System

NEA has an agreement with the U.S. Department of Transportation (DOT) to utilize the Enterprise Service Center's (ESC) Oracle Federal Financial System, Delphi, as their financial management system. OMB requires that such service organizations provide client agencies with an independent report describing system controls. To comply with this requirement, DOT OIG hired an independent contractor, Clifton Gunderson, LLP, to conduct a review on the computer controls over the information technology and data processing environment, as well as the input processing, and output controls built into the Delphi system.

The independent contractor rendered an opinion on the effectiveness of those controls for the nine-month period from October 1, 2008 through June 30, 2009. The audit concluded that "management presented its description of ESC controls fairly in all material respects" and that "controls, as described, were suitably designed for all stated control objectives." In addition, controls "were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified by management were achieved from October 1, 2008, through June 30, 2009. The exceptions are ineffective access controls and segregation of duties concerning the CASTLE[1] system operations." CASTLE is used to support DOT operations only.

[1] Consolidated Automated System for Time and Labor Entry (CASTLE).

Payroll System

NEA uses the U.S. Department of Agriculture (USDA) National Finance Center as its payroll provider. In September 2009, the USDA OIG issued its Statement on Auditing Standards Number 70 Report, *Review of the Department of Agriculture Office of the Chief Financial Officer/National Finance Center (OCFO/NFC).* The review concluded that the OCFO/NFC's "description of controls presented fairly, in all material respects, the relevant aspects of OCFO/NFC." Also, in their opinion, "the controls included in the description were suitably designed and operating with sufficient effectiveness to provide reasonable assurance that associated control objectives would be achieved if customer agencies and subservice organizations applied the controls contemplated in the design of NFC's controls." There were no recommendations in the report.

EXIT CONFERENCE

An exit conference was held with ITM officials on January 14, 2010. The officials generally concurred with our findings and recommendations and agreed to initiate corrective actions.

RECOMMENDATIONS

We recommend that the NEA Office of Information and Technology Management:

1. Complete corrective actions for Recommendation No. 2 in the FY 2008 FISMA Evaluation. *ITM should provide the OIG a completed and approved COOP*.

2. Complete and approve the Security Plan as required by its *Standard Procedures for Developing Information Technology Policies.* A copy of the approved Security Plan should be provided to the OIG.

3. Implement its standard procedures for developing all policies as required by the "Standard Procedures for Developing Information Technology Policies," make those policies available to employees.

4. Perform the security certification and accreditation review on all its systems as required and update its C&A policy to reflect current ITM and federal requirements.

5. Include all *Plans of Action and Milestones* (POA&Ms), which are more than *90* days beyond the planned remediation date, in its quarterly FISMA report as required by the Office of Management and Budget.

6. Develop policies and implement procedures to ensure that the ITM inventory is completed annually.

7. Approve and implement the *NEA Change Management Policy/Procedure* as required by its *Standard Procedures for Developing Information Technology Policies.*